418 Rec'd PCT/PTO 10 FEB 2000

13 Rec'd PCT/PTO 07 FEB 2000

FORM PTO-1390
(REV. 5-93)

U S DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER
2345/115

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

U S. APPLICATION NO (If known, see 37 CFR 1.5)
09/485408

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED:
PCT/EP98/04424 ✓	(16.07 98) 16 July 1998 ✓	(06.08.97) 06 August 1997 ✓

TITLE OF INVENTION
TRANSCODER FOR DECODING ENCODED TV PROGRAMS ✓

APPLICANT(S) FOR DO/EO/US
WILHELM, Siegfried and KOWALSKI, Bernd ✓

Applicants herewith submit to the United States Designated/Elected Office (DO/EO/US) the following items and other information

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C 371.
3. ☒ This is an express request to begin national examination procedures (35 U S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U S.C 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U S.C. 371(c)(4)).
10. ☒ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C 371(c)(5))

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A **FIRST** preliminary amendment.
    ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment
14. ☒ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information: Preliminary Examination Report and International Search Report.

EXPRESS MAIL NO. EL179105317

PTO/PTO 10 FEB 2000

U.S. APPLICATION NO (if known, see 37 C.F.R.1.5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
09/485408	PCT/EP98/04424	2345/115

17. ☒ The following fees are submitted:	CALCULATIONS | PTO USE ONLY	
Basic National Fee (37 CFR 1.492(a)(1)-(5)):		
Search Report has been prepared by the EPO or JPO $840.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) . . . $670.00		
No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1 445(a)(2)) . . $760.00		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO $970.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) $96.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 840	
Surcharge of $130 00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

Claims	Number Filed	Number Extra	Rate		
Total Claims	13 - 20 =	0	X $18.00	$ 0	
Independent Claims	3 - 3 =	0	X $78.00	$ 0	
Multiple dependent claim(s) (if applicable)			+ $260.00	$ 0	
TOTAL OF ABOVE CALCULATIONS =				$ 840	
Reduction by ½ for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 CFR 1.9, 1 27, 1.28).				$	
SUBTOTAL =				$ 840	
Processing fee of $130.00 for furnishing the English translation later the ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +				$	
TOTAL NATIONAL FEE =				$ 840	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). $40.00 per property +				$	
TOTAL FEES ENCLOSED =				$ 840	
				Amount to be: refunded	$
				charged	$

a. ☐ A check in the amount of $_____ to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No 11-0600 in the amount of **$ 840.00** to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 11-0600. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

By: Lisa Magnotta (Reg. No. 41,172)

Richard L. Mayer
SIGNATURE

SEND ALL CORRESPONDENCE TO:

Kenyon & Kenyon
One Broadway
New York, New York 10004

Richard L. Mayer, Reg. No. 22,490
NAME

2/7/00
DATE

254808

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT: WILHELM et al.

SERIAL NO.: to be assigned

FILED: herewith

TITLE: TRANSCODER FOR DECODING ENCODED TV PROGRAMS

ART UNIT: not yet known

EXAMINER: not yet known

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

PRELIMINARY AMENDMENT

Please amend the above-identified application before a first consideration on the merits as follows:

IN THE DRAWINGS

Please replace Figs. 1-4 with replacement Figs. 1-4 submitted herewith.

IN THE ABSTRACT

Please replace the Abstract with the replacement Abstract submitted herewith.

IN THE SPECIFICATION

Please replace the specification with the attached substitute specification. Also submitted herewith is a marked-up copy of the specification. No new matter has been added.

EL179105317

IN THE CLAIMS

On the first page of the claims, line 1, change "Patent Claims" to --WHAT IS CLAIMED IS:--.

Please cancel without prejudice original claims 1-14 and cancel the substitute claims 1-12 annexed to the International Preliminary Examination Report. Please also add new claims 15-27 as follows:

--15 . (new) A decoder device for decrypting encrypted television programs, the decoder device comprising:

a control unit;

an input for receiving the encrypted television program;

a decryption device for decrypting the encrypted television program into a format reproducible by a television set;

an output capable of being connected to the television set so as to output the decrypted television program to the television set for reproduction;

a first interface for interfacing to at least one of a first identification and a first key carrier component for enabling the decryption device, the first interface being disposed in the control unit;

a second interface for interfacing to the control unit;

a third interface for interfacing to a telecommunications network; and

a fourth interface for interfacing to at least one of a second identification and a second key carrier component, an authorization by at least one of the second identification and the second key carrier component being useable for establishing a connection to a subscriber via the telecommunications network.

16. (new) The decoder device as recited in claim 15 wherein the fourth interface is disposed in the control unit.

17. (new) The decoder device as recited in claim 15 wherein the television set includes a fifth interface for receiving control commands and wherein the control unit is capable of controlling the television set.

18. (new) The decoder device as recited in claim 15 wherein the first and the second identification and/or key carrier components include a respective smart card or a common smart card.

19. (new) The decoder device as recited in claim 15 further comprising a sixth interface for connecting the decoder device to a computer, the computer being adaptable for at least one of controlling the decoder device and establishing a connection to a subscriber via the telecommunications network.

20. (new) The decoder device as recited in claim 15 wherein the control unit includes a computer, the computer including a seventh interface for controlling the decoder device and including the first and fourth interfaces.

21. (new) The decoder device as recited in claim 15 wherein the decoder device is integrated in the television set.

22. (new) A smart card for a decoder device, the decoder device including a decryption device for decrypting the encrypted television program into a format reproducible by a television set, a control unit and a first interface for interfacing to a first identification and/or key carrier component and for enabling the decryption device, the first interface being disposed in the control unit, the smart card comprising:

a computer unit;

at least one peripheral device;

a first memory area, the first memory area being subdivided into at least a protected area and an unprotected area, an access to the protected area being a function of a check for permitted access, a general key being stored in the protected area, an external host computer being useable to enter at least one simple key and a protocol program associated with the at least one simple key under a control of the general key; and

a second memory area for storing at least parts of an operating system capable of controlling communication between the computer unit and the at least one peripheral and communication with an external host computer and capable of managing at least one of the protected and unprotected memory areas of the first memory area.

23. (new) The smart card as recited in claim 22 wherein the first memory area is further subdivided into a read/write memory area and wherein the operating system is capable of managing at least one of the read/write, the protected and the unprotected memory areas of the first memory area.

24. (new) The smart card as recited in claim 22 wherein the second memory area is capable of storing a key management useable for access to a protocol program of the at least one simple key.

25. (new) A method for a host computer of a pay TV provider to communicate with a decoder device and a smart card, the decoder device including a control unit and a decryption device for decrypting a encrypted television program into a format reproducible by a television set, the smart card including a protected memory area, a general key being stored in the protected area, the method comprising:

establishing a telecommunications connection between the host computer and the decoder device using the host computer;

checking the general key in the smart card using the host computer;

when a result of the checking is positive, communicating a simple key and a protocol program associated with the key to the smart card in encrypted form;

entering the simple key and the protocol program into the protected memory area of the smart card; and

inhibiting the protected memory area of the smart card.

26. (new) The method as recited in claim 25 wherein the smart card includes a computer unit and further comprising decrypting the key and the protocol program using the computer unit before the entering step.

27. (new) The method as recited in claim 25 wherein the decoder device further includes a first interface with a telecommunications network and the television set includes a second interface with an antenna for receiving the encrypted television program and further comprising transmitting a first data transmission traffic via the first interface and transmitting a second data transmission traffic via the second interface, the transmitting of the first and

second data transmissions being performed together with or prior to a useful signal that reproduces the encrypted television program, information for the first and second data transmissions being distributed and transmitted so that the information is capable of being decrypted in only an alternating manner and in only a step-by-step manner.--.

REMARKS

Due to the large number of amendments to the original specification necessary, a substitute specification, along with a marked-up copy of the original specification in accordance with 37 C.F.R. § 1.125, is submitted herewith. It is respectfully submitted that no new matter has been added. This Preliminary Amendment cancels original claims 1-14 in the underlying PCT Application No. PCT/EP98/04424 and the substitute claims 1-12 annexed to the International Preliminary Examination Report (a translation of which is submitted herewith), and adds new claims 15-27. The new claims do not add new matter to the application but do conform the claims to U.S. Patent and Trademark Office rules.

The amendments to the specification, abstract and drawings are to conform the specification, abstract and drawings to U.S. Patent and Trademark Office rules. It is respectfully submitted that the amendments to the specification, abstract and drawings do not introduce new matter into the application.

The underlying PCT application includes a Search Report, a copy of which is included herewith.

Conclusion

Consideration of the present application as amended is hereby respectfully requested.

Respectfully Submitted,

Kenyon & Kenyon

By: Des Magat (Reg. No 41,172)

Dated: 2/7/00

By: Erik Swanson

Erik R. Swanson
(Reg. No. 40,833)

One Broadway
New York, NY 10004
Tel. (212) 425-7200
Fax. (212) 425-5288

Abstract

The invention pertains to a transcoder provided with a control unit and intended for decoding encoded TV programs. Said transcoder has an input for entering an encoded TV program, a decoding device for decoding an encoded TV program into a format which can be played on a television set, an output which can be connected to said television set and is designed to enter the encoded TV program into the television set for play, an interface for an identification or key component, to be used for validation of the decoding device, as well as an interface for a control unit in the transcoder. The transcoder according to the invention is characterzied in that the interface for the identification or key component is located in said control unit.

[2345/115]

DECODER DEVICE FOR DECRYPTING ENCRYPTED TELEVISION PROGRAMS

Field of the Invention

The present invention relates to a decoder device for decrypting encrypted television programs. In particular, the present invention relates to a decoder device having a control unit, for the decryption of encrypted television programs, having an input for feeding in an encrypted television program, a decryption device, which decrypts an encrypted television program into a format that can be reproduced by a television receiver, an output, which can be connected to a television receiver in order to feed the decrypted television program into the television receiver for reproduction, an interface for an identification and/or key carrier component for enabling the decryption device, and an interface for a control unit of the decoder device.

Related Technology

A decoder device for decrypting encrypted television programs enables the reception and decryption of so-called pay TV programs, present-day decoder devices being commercially available as so-called set-top boxes for conventional television receivers.

The invoicing that has been customary heretofore, for example monthly invoicing, for supplying programs in pay TV is shifting more and more to an individual ("pay-per-view") invoicing practice. Therefore, there is a need to identify and authenticate the program customer before the program customer accesses the program. In addition, in the case of so-called HOT programs (home order television), the program customer's orders are also debited to said customer's bank account or his credit on a smart card. Here, too, it is necessary to identify and authenticate the program customer and, when needed, implement security mechanisms to protect against misuse.

EL179105 317

To secure electronic invoicing processes, and to protect confidential information (bank account data, account balances, etc.), use is made of smart cards having microprocessors which are equipped with encryption algorithms. An encryption algorithm of this type is the so-called RSA algorithm. In the case of pay TV, a smart card of this type is part of the so-called "conditional access system" (CAS), which is used to check whether the person making the inquiry is actually the authorized program customer and, if applicable, whether his creditworthiness suffices for the desired service. In so-called "electronic commerce", as well, this smart card represents the identity of the customer or of his electronic purse. In this context, a replenishable credit can be recorded on the smart card. The smart card is generally accessed, in a more or less automated manner, by third parties (program providers, commercial entities or the like), via telephone or the internet, using the set-top box before or during the transaction.

A growing problem in this connection is the rising number of program or service providers which a program customer can subscribe to via these media. The result is an ever increasing outlay for equipment (set-top box, television set, internet terminal (PC or net PC), remote control units for the set-top box and the television set, as well as an ever increasing number of smart cards needed to utilize the individual services.

Summary of the Invention

An object of the present invention is, therefore, to provide these various components less expensively, i.e., to reduce their hardware outlay, and so that they are less susceptible to faults and simpler for the program customer to handle. Moreover, the present invention addresses the problem of security which is becoming increasingly relevant, in connection with services being utilized by unauthorized third parties.

The present invention provides a decoder device which includes an interface for the identification and/or key carrier component in the control unit of the device.

This design makes it possible to reduce the number of interfaces. Moreover, the

program customer (user) is able to carry out his transactions in a more convenient manner, since the control unit of the decoder device is already equipped with a keypad in any case. Furthermore, security is improved, since the program customer (even among a relatively large number of third parties) can effect his inputs (PIN, TAN, etc.) without third parties being able to observe this. Moreover, the control unit of the decoder device can be kept securely, together with the identification and/or key carrier component (smart card), whereas, as a rule, for the sake of convenience, a smart card is not removed from the decoder device (set-top box).

In accordance with one preferred embodiment of the decoder device having a control unit in accordance with the present invention, the control unit is also set up for controlling the television receiver set, which has an interface for receiving control commands from the control unit. This constitutes a further reduction in equipment outlay. Moreover, overall access to the television receiver set can be controlled. In other words, even television use for programs that do not involve payment must be enabled by the authorized user. This can be achieved by having the function of the control unit as a whole depend on the authorized user inputting the identifier (PIN).

In order for the program provider to handle debiting and to identify the program customer, in the case of the decoder device according to the present invention, use is made, in particular, of an interface to a telecommunications network. This can be a modem, or a corresponding coupling device for digital telecommunications networks.

In particular, to enhance security in the system, an interface to an identification and/or key carrier component is used. Via such an interface to a telecommunications network, the program customer can make contact with a service provider or merchandise shipper. Here as well, a connection to a specific subscriber (service provider or merchandise shipper) via the telecommunications network is established as a function of an authorization by the identification and/or key carrier component. The program provider is thus considered independently of the service provider or merchandise shipper, when the program customer is invoiced. This can be

advantageous with respect to data security and flexibility.

Alternatively, however, it is also possible that the program provider and the service provider cooperate in a suitable fashion, making it possible to have a shared invoicing and/or customer administration, as well as customer identification and customer authorization. In such a case, there is no need for separate smart cards.

At any rate, it is advantageous for the interface to the identification and/or key carrier component for the authorization of the connection via the telecommunications network to also be arranged in the control unit.

As already mentioned, the identification and/or key carrier component for the authorization of the connection via the telecommunications network and the identification and/or key carrier component for enabling the decryption device can be implemented either by two separate or by one common smart card.

In a further refinement, the decoder device is provided with an interface for connecting the decoder device to a computer, which is set up for controlling the decoder device and/or for establishing a connection to another subscriber via the telecommunications network. It is, thus, possible to make available to the program customer the entire functionality of a computer (PC or internet PC), i.e., the storing and processing of data and information, as well as the more convenient configuration of dialogs between the program customer and, for example, the program provider or the service provider.

In one embodiment of the present invention, the control unit is formed by the computer, which has an interface for controlling the decoder device, and an interface for the identification and/or key carrier component for authorizing the connection via the telecommunications network and/or the identification and/or key carrier component for enabling the decryption device. This eliminates the need for one or two separate control units. It goes without saying that in this specific embodiment as

well, the two smart cards for the traffic with the program provider and the service provider can also be realized as one common smart card.

It should also be mentioned that the connection between the computer and the television set, or the computer and the decoder device, can either be wire-free (for example, an infrared or ultrasonic connection) or wire-based. In addition, the not very stringent demands placed on the computer (relatively small memory, no need for an especially ergonomic keyboard due to mostly short inputs, etc.), mean that a so-called palmtop design is possible, with the appropriate interfaces (infrared interface to the decoding device of one such or more interfaces for the smart card(s)). Thus, the user is able to control and operate his equipment in a very compact and convenient manner, and also simply and conveniently communicate with the program provider and/or the service/merchandise provider. Finally, there is also a substantial reduction in the outlay for cabling between the individual components at the user end, which likewise enhances the convenience.

One embodiment of the present invention provides for the decoder device to be integrated in the television set. The user is thus provided with a self-contained apparatus which is especially protected against misuse, and in which all of the functions (conventional television, pay TV, communication with a service/merchandise provider via the telecommunications network, storage and/or post-processing of the received data in the computer, etc.) can be performed in a manner in which they are protected from misuse.

The present invention also provides a smart card for an above-described decoder device with a control unit, having a computer unit, a first memory area, in which are stored at least parts of operating system functions which are used to control the communication between the computer unit of the smart card and the peripherals of the smart card, as well as the communication with an external host computer, and which are used to manage protected, unprotected and/or read/write memory areas of the smart card, and having a second memory area, which is subdivided into protected and

unprotected areas, access to protected areas being made as a function of a check for permitted access, a general key being stored in the protected area of the second memory area, and under the control of the general key, the external host computer entering at least one further simple key, as well as a protocol program associated with this further simple key.

This smart card makes it possible for the decoder device described above to be operated quite securely and also simply, thereby expanding the access to a plurality of additional service providers.

Preferably stored in the second memory area is a key management, from which access is made to a protocol program of a simple key.

In this context, the following method according to the present invention is used to supplement additional keys, i.e., ways of accessing additional providers:

- a telecommunications connection is established by the host computer between the host computer and the decoder device with the control unit or the computer containing the control unit;
- the host computer checks the general key in the smart card;
- a simple key, as well as a protocol program associated with the key are communicated to the smart card in encrypted form, in the case that the check test has a positive result;
- the simple key and the protocol program associated with the key are entered into the protected memory area of the smart card; and
- the protected memory area of the smart card is inhibited.

In this context, before the simple key and the protocol program associated with the key are entered into the protected memory area of the smart card, the key and the protocol program can be decrypted by the computer unit of the smart card.

Brief Description of the Drawings

Figure 1 shows a prior art decoder device arrangement in a schematic block diagram; and

Figures 2 through 4 show various embodiments of a decoder device arrangement according to the present invention, each in a schematic block diagram.

Detailed Description

Figure 1 illustrates terminal environment for combined pay TV and electronic commerce applications that is customary today. The broadband, digitally encrypted pay TV useful signal is received by the television set 10 via line 1 and transferred via output 4 to input IN (not shown), into set-top box (STB) 12. There, the signal is decrypted by a special chip using an algorithm provided for this - the DVB algorithm is mentioned here as being representative of all such algorithms - and retransmitted to the television set. The keys are set by a smart card (ICC DVB) 14 via interface 3. The smart card contains the key-distribution algorithm of the conditional access system (e.g. RSA) and the customer's secret key. Only a customer having a valid smart card 14 is able to decrypt pay TV broadcasts. The smart card 14 is connected to set-top box 12 via smart card interface (IFD) 16.

Enhancements to set-top box 12 envisage connecting a backward channel via the telephone network or internet via interface 5 to the servers of various service providers, e.g., for ordering services or goods advertised on the pay TV channels. To safeguard the order and payment, a second smart card (ICC BC) 18 can be inserted in this case via a further interface (IFD) 20, establishing connection 6 between second smart card 18 and second interface 20.

Other possible enhancements for linking set-top box 12 envisage using an IR remote control 22 via interface 9 and a computer (PC) 24 via an interface 7 that is customary in the PC environment, referred to here simply as "PCI" (e.g., V24/RS232C or parallel interface). The computer 24 facilitates, for example, user-friendly backward channel

transactions or the post-processing of information from the pay TV channels.

There are various ways to connect smart cards 14 and 18 to set-top box 12. Either smart card interfaces 16 and 20 are permanently installed in set-top box 12, or they are designed to be insertable as PCMCIA modules. PCMCIA modules make it possible to exchange one pay TV access method (CAS) for another without any intervention in set-top box 12.

Disadvantages associated with conventional terminal configurations include the lack of user-friendliness, the elaborate cabling of set-top box 12, and its complicated interface configuration.

Specific embodiments of the present invention are illustrated in Figures 2, 3 and 4.

Referring now to Fig. 2, the remote controls of set-top box 32 and of television set (TV set) 30 are combined in one device, control unit (RCU) 42, already in a first integration stage. The new control unit 42 receives a smart card interface 34, capable of driving both smart card (ICC DVB) 38of the pay TV system, as well as smart card (ICC BC) 40 of the backward channel. In terms of the functional sequence, the key exchange of the conditional access system (CAS) of the pay TV is carried out exactly as in the conventional configuration.

In Figure 2, however, an IR interface 37 links smart card 38 via control unit 34 to the pay TV decryption chip 42 (e.g., DVB) in set-top box 32. The same applies to smart card 40, which, at this point, likewise safeguards the backward channel via control unit 34 and its IR interface.

It is, therefore, no longer necessary to insert smart cards into set-top box 32, eliminating the need for any smart card interfaces at the set-top box 32. The customer inserts his cards directly into the remote control 34. If pay TV providers and backward channel service providers agree contractually to this effect, then the

functions of both smart cards 38 and 40 can even be combined on a single smart card (ICC).

In Figure 2, the computer (PC) 41 either continues to be connected to set-top box 32 via a conventional interface (PCI) 42 or likewise utilizes the IR interface (infrared interface) 44 of set-top box 32 for this purpose.

The backward channel connection to the telecommunications network is effected either via set-top box 32 or via the computer 41. Both variants are possible in principle.

Figure 3 shows remote control (RCU) and computer (PC) combined in a further integration stage into a combined apparatus (RCU/PC) 50. Here, one can utilize the advantages of the computer PC and of remote control (RCU) simultaneously. This approach is of particular interest when the combined apparatus 50 is similar to a "network PC" and can be operated compactly and without complicated peripherals and cabling, e.g., from the coffee table.

Figure 4 illustrates the television set (TV set) and set-top box (STB) combined in just one terminal 70, as a further integration stage.

The new terminal configurations illustrated in Figures 2 through 4 show how one can appreciably simplify the operation and cabling of the terminals without degrading functionality.

Therefore, in accordance with the present invention, instead of one or more smart card interfaces on the set-top box (STB), the relevant smart cards are now connected via a remote control (RCU) 76 and its infrared interfaces 78 to the pay TV decryption chip remaining in set-top box 70. Thus, the need is eliminated for costly and delicate interfaces on the set-top box.

Moreover, the functions of the pay TV smart card and of the backward-channel smart card can be combined in a user-friendly manner on just one card, with the assistance of a special remote control RCU.

Finally, combining the remote control and the PC in combined apparatus 76 makes it possible to move the backward channel connection out of the set-top box 70. This makes it possible to optimally utilize an internet PC (a PC which is linked via any desired online networks to servers of any desired service providers), in conjunction with pay TV services, including their backward channel options.

A further aspect of the present invention is configuring the smart card so that it, too, can handle, with a high level of security, both the decryption of the program of the pay TV provider and transactions (ordering and payment of purchase price) with the goods/service provider.

In particular, if further goods/service providers are added over time, this means in each case that the program customer needs a new smart card containing the keys and protocols of the previous providers (both pay TV providers and goods/service providers) and the key and the protocol of the newly added provider.

The present invention likewise provides an approach for this:
Since the goods/service provider is linked in any case, as a rule, to the user by the same host computer as the pay TV provider, this host can also access the inhibited areas of the customer's smart card by a general key, in order to store there a further key and the associated protocol for future transactions (decryption or payment processes).

Moreover, a vector table or an interrogation routine, in which the newly added keys are successively managed, is to be executed in an additional area (possibly likewise inhibited). In response to a smart card access, it is first checked on the basis of the vector table or the interrogation routine to see whether an appropriate key is present,

or whether the key input by the user matches one of the keys stored on the smart card. Only when this interrogation has a positive result, is the program associated with the respective key (if indicated, decrypted and then) executed for the purpose of transaction or decryption.

The key and the associated protocol (program) are preferably likewise transmitted in an encrypted form, from the host computer to the set-top box 32, 70 and, from there, routed via the interface to the control unit 34, 50, 76. When the control unit is integrated with computer (PC) as combined apparatus 50, 76, the host computer can be directly linked to the computer (PC) via the telecommunications network 48, 68, 88, to transmit the information for, or into, smart card 38, 40, 72, 74.

Depending on the specific configuration, it is possible for the protocol (program) to be stored in the smart card just in an encrypted form, and for it to be decrypted in each case for the delay prior to execution. Alternatively, however, the protocol (program) can also be rendered in an executable form when it is stored in the (protected) memory area of the smart card.

As a result, the memory of the smart card contains (inter alia) the following programs and/or data:

An operating system core for controlling communications between the smart card processor and the peripherals on the smart card, as well as communications with the host computer which manages the memory areas of the smart card (protected and unprotected areas, read/write areas, flash EEPROM, etc.), etc. Keys (a master or general key, and also one or more application keys), the master key being used to transfer (further) application keys and the associated application or protocol programs into the memory area. The application keys ensure that the protocol programs are executed (and thus orders handled or pay TV programs decrypted) only in response to proper user input.

Encrypted user programs or protocol programs for controlling the handling of orders or the decryption of pay TV programs.

To enhance security, provision is made for the identification and authentication between the control unit 34, 50, 76 and/or the set-top box 32, 70 or television set 30, 70, on the one hand, and the host computer, on the other hand, to be carried out on different routes or channels. In other words, some of the protocol traffic is transmitted via interface 5 to the telecommunications network 48, 68, 88, and some via line 1, together with or prior to the broadband, digitally encrypted pay TV useful signal. In this context, the enabling/inhibiting of services can also take place on these routes. Since a case of misuse would require synchronously intercepting and decrypting both channels, security is thus considerably higher. In particular, information can be distributed between the two channels at the time of enabling/inhibiting, or of new keys, etc., in such a way that it is able to be decrypted only in an alternating and also only in a step-by-step manner, in each instance, with knowledge thereof.

[2345/115]

DECODER DEVICE FOR DECRYPTING ENCRYPTED {
}TELEVISION PROGRAMS

[Field of the Invention

The present] ~~{The }~~ invention relates to a decoder device for decrypting encrypted television programs. In particular, the present invention relates to a decoder device having a control unit, for the decryption of encrypted television programs, having an input for feeding in an encrypted television program, a decryption device, which decrypts an encrypted television program into a format that can be reproduced by a television receiver, an output, which can be connected to a television receiver in order to feed the decrypted television program into the television receiver for reproduction, an interface for an identification and/or key carrier component for enabling the decryption device, and an interface for a control unit of the decoder device.

[Related Technology]

A decoder device ~~{of this type}~~ **[for decrypting encrypted television programs]** enables the reception and decryption of so-called pay TV programs, present-day decoder devices being commercially available as so-called set-top boxes for conventional television receivers.

The invoicing that has been customary heretofore, for example monthly invoicing, for supplying programs in pay TV is shifting more and more to an individual ("pay-per-view") invoicing practice. Therefore, there is a need to identify and authenticate the program customer before the program customer accesses the program. In addition, in the case of so-called HOT programs (home order television), the program customer's orders are also debited to said customer's bank account or his credit on a smart card. Here, too, it is necessary to identify and authenticate the program customer and, when needed, implement security mechanisms to protect against misuse.

EL179105317

To secure electronic invoicing processes, and to protect confidential information (bank account data, account balances, etc.), use is made of smart cards having microprocessors which are equipped with encryption algorithms. An encryption algorithm of this type is the so-called RSA algorithm. In the case of pay TV, a smart card of this type is part of the so-called "conditional access system" (CAS), which is used to check whether the person making the inquiry is actually the authorized program customer and, if applicable, whether his creditworthiness suffices for the desired service. In so-called "electronic commerce", as well, this smart card represents the identity of the customer or of his electronic purse. In this context, a replenishable credit can be recorded on the smart card. The smart card is generally accessed, in a more or less automated manner, by third parties (program providers, commercial entities or the like), via telephone or the internet, using the set-top box before or during the transaction.

A growing problem in this connection is the rising number of program or service providers which a program customer can subscribe to via these media. The result is an ever increasing outlay for equipment (set-top box, television set, internet terminal (PC or net PC), remote control units for the set-top box and the television set, as well as an ever increasing number of smart cards needed to utilize the individual services.

[Summary of the Invention

An] ~~{The}~~ object of the present invention is, therefore, to ~~{design}~~ **[provide]** these various components ~~{to be}~~ less ~~{expensive}~~ **[expensively]**, i.e., to reduce their hardware outlay, and ~~{to design them to be}~~ **[so that they are]** less susceptible to faults and simpler for the program customer to handle. Moreover, the present invention ~~{intends to consider}~~ **[addresses]** the problem of security which is becoming increasingly relevant, in connection with services being utilized by unauthorized third parties.

~~{This objective is achieved in accordance with the present invention by configuring~~

~~the~~ **[The present invention provides a decoder device which includes an]** interface for the identification and/or key carrier component in the control unit of the ~~{decoder}~~ device.

This design makes it possible to reduce the number of interfaces. Moreover, the program customer (user) is able to carry out his transactions in a more convenient manner, since the control unit of the decoder device is **[already]** equipped with a keypad in any case. Furthermore, security is improved, since the program customer (even among a relatively large number of third parties) can effect his inputs (PIN, TAN, etc.) without third parties being able to observe this. Moreover, the control unit of the decoder device can be kept securely, together with the identification and/or key carrier component~~{,}~~ (smart card), whereas, as a rule, for the sake of convenience, a smart card is not removed from the decoder device ~~{(=}~~[(]set-top box).

In accordance with one preferred embodiment of the decoder device having a control unit in accordance with the present invention, the control unit is also set up for controlling the television receiver set, which has an interface for receiving control commands from the control unit. This constitutes a further reduction in equipment outlay. Moreover, overall access to the television receiver set can be controlled. In other words, even television use for programs that do not involve payment must be enabled by the authorized user. This can be achieved by having the function of the control unit as a whole depend on the authorized user inputting the identifier (PIN).

In order for the program provider to handle debiting and to identify the program customer, in the case of the decoder device according to the present invention, use is made, in particular, of an interface to a telecommunications network. This can be a modem, or a corresponding coupling device for digital telecommunications networks.

In particular, to enhance security in the system, an interface to an identification and/or key carrier component is used. Via such an interface to a telecommunications network, the program customer can make contact with a service provider or

merchandise shipper. Here as well, a connection to a specific subscriber (service provider or merchandise shipper) via the telecommunications network is established as a function of an authorization by the identification and/or key carrier component. The program provider is thus considered independently of the service provider or merchandise shipper, when the program customer is invoiced. This can be advantageous with respect to data security and flexibility.

Alternatively, however, it is also possible that the program provider and the service provider cooperate in a suitable fashion, making it possible to have a shared invoicing and/or customer administration, as well as customer identification and customer authorization. In such a case, there is no need for separate smart cards.

At any rate, it is advantageous for the interface to the identification and/or key carrier component for the authorization of the connection via the telecommunications network to also be arranged in the control unit.

As already mentioned, the identification and/or key carrier component for the authorization of the connection via the telecommunications network and the identification and/or key carrier component for enabling the decryption device can be implemented either by two separate or by one common smart card.

In a further refinement, the decoder device is provided with an interface for connecting the decoder device to a computer, which is set up for controlling the decoder device and/or for establishing a connection to another subscriber via the telecommunications network. It is, thus, possible to make available to the program customer the entire functionality of a computer (PC or internet PC), i.e., the storing and processing of data and information, as well as the more convenient configuration of dialogs between the program customer and, for example, the program provider or the service provider.

In one ~~{especially preferred specific}~~ embodiment of the present invention, the

control unit is formed by the computer, which has an interface for controlling the decoder device, and an interface for the identification and/or key carrier component for authorizing the connection via the telecommunications network and/or the identification and/or key carrier component for enabling the decryption device. This eliminates the need for one or two separate control units. It goes without saying that in this specific embodiment as well, the two smart cards for the traffic with the program provider and the service provider can also be realized as one common smart card.

It should also be mentioned that the connection between the computer and the television set, or the computer and the decoder device, can either be wire-free (for example, an infrared or ultrasonic connection) or wire-based. In addition, the ~~{special}~~ **[not very stringent]** demands placed on the computer (relatively small memory, no need for an especially ergonomic keyboard due to mostly short inputs, etc.), mean that a so-called palmtop design is possible, with the appropriate interfaces (infrared interface to the decoding device of one such or more interfaces for the smart card(s)). Thus, the user is able to control and operate his equipment in a very compact and convenient manner, and also simply and conveniently communicate with the program provider and/or the service/merchandise provider. Finally, there is also a substantial reduction in the outlay for cabling between the individual components at the user end, which likewise enhances the convenience.

One ~~{especially preferred specific}~~ embodiment of the present invention provides for the decoder device to be integrated in the television set. The user is thus provided with a self-contained apparatus which is ~~{specially}~~ **[especially]** protected against misuse, and in which all of the functions (conventional television, pay TV, communication with a service/merchandise provider via the telecommunications network, storage and/or post-processing of the received data in the computer, etc.) can be performed in a manner in which they are protected from misuse.

The present invention also ~~{relates to}~~ **[provides]** a smart card for an above-described

decoder device with a control unit, having a computer unit, a first memory area, in which are stored at least parts of operating system functions which are used to control the communication between the computer unit of the smart card and the peripherals of the smart card, as well as the communication with an external host computer, and which are used to manage protected, unprotected and/or read/write memory areas of the smart card, and having a second memory area, which is subdivided into protected and unprotected areas, access to protected areas being made as a function of a check for permitted access, a general key being stored in the protected area of the second memory area, and under the control of the general key, the external host computer entering at least one further simple key, as well as a protocol program associated with this further simple key.

This smart card makes it possible for the decoder device described above to be operated quite securely and also simply, thereby expanding the access to a plurality of additional service providers.

Preferably stored in the second memory area is a key management, from which access is made to a protocol program of a simple key.

In this context, the following method according to the present invention is used to supplement additional keys, i.e., ways of accessing additional providers:

- a telecommunications connection is established by the host computer between the host computer and the decoder device with the control unit or the computer containing the control unit;
- the host computer checks the general key in the smart card;
- a simple key, as well as a protocol program associated with the key are communicated to the smart card in encrypted form, in the case that the check test has a positive result;
- the simple key and the protocol program associated with the key are entered into the protected memory area of the smart card; **[and]**
- the protected memory area of the smart card is inhibited.

In this context, before the simple key and the protocol program associated with the key are entered into the protected memory area of the smart card, the key and the protocol program can be decrypted by the computer unit of the smart card.

[Brief Description of the Drawings]

Figure 1 shows a ~~{related-}~~**[prior]** art **[decoder device]** arrangement in a schematic block diagram**[; and]**~~{.}~~

Figures 2 ~~{- 4 depict}~~ **[through 4 show]** various ~~{specific}~~ embodiments of **[a decoder device arrangement according to]** the present invention, each in a schematic block diagram.

[Detailed Description]

Figure 1 illustrates terminal environment for combined pay TV and electronic commerce applications that is customary today. The broadband, digitally encrypted pay TV useful signal is received by the television set **[10]** via line ~~{(1)}~~ **[1]** and transferred via output ~~{(4)}~~ **[4]** to input ~~{(IN)}~~ **[IN (not shown)]**, into set-top box (STB) **[12]**. There, the signal is decrypted by a special chip using an algorithm provided for this - the DVB algorithm is mentioned here as being representative of all such algorithms - and retransmitted to the television set. The keys are set by a smart card (ICC DVB) **[14]** via interface ~~{(3)}~~ **[3]**. The smart card contains the key-distribution algorithm of the conditional access system (e.g. RSA) and the customer's secret key. Only a customer having a valid smart card ~~{(ICC DVR)}~~ **[14]** is able to decrypt pay TV broadcasts. The smart card ~~{(ICC DVR)}~~ **[14]** is connected to set-top box ~~{(STB)}~~ **[12]** via smart card interface ~~{"IFD"}~~**[(IFD) 16]**.

Enhancements to set-top box ~~{(STB)}~~ **[12]** envisage connecting a backward channel via the telephone network or internet via interface ~~{(5)}~~ **[5]** to the servers of various service providers, e.g., for ordering services or goods advertised on the pay TV channels. To safeguard the order and payment, a second smart card (ICC BC) **[18]** can be inserted in this case via a further interface (IFD) **[20]**, establishing connection ~~{(6)}~~ **[6]** between second smart card ~~{(ICC BC)}~~ **[18]** and second interface ~~{(IFD)}~~

[20].

Other possible enhancements for linking set-top box ~~{(STB)}~~ **[12]** envisage using an IR remote control ~~{(9)}~~ **[22 via interface 9]** and a computer ~~{PC}~~**[(PC) 24]** via an interface ~~{(7)}~~ **[7]** that is customary in the PC environment, referred to here simply as "PCI" (e.g., V24/RS232C or parallel interface). The computer ~~{PC}~~ **[24]** facilitates, for example, user-friendly backward channel transactions or the post-processing of information from the pay TV channels.

There are various ways to connect ~~{two}~~ smart cards **[14 and 18]** to set-top box ~~{(STB)}~~ **[12]**. Either smart card ~~{terminals (IFD)}~~ **[interfaces 16 and 20]** are permanently installed in set-top box ~~{(STB)}~~ **[12]**, or they are designed to be insertable as PCMCIA modules. PCMCIA modules make it possible to exchange one pay TV access method (CAS) for another without any intervention in set-top box ~~{(STB)}~~ **[12]**.

Disadvantages associated with conventional terminal configurations include the lack of user-friendliness, the elaborate cabling of set-top box ~~{(STB)}~~ **[12]**, and its complicated interface configuration.

Specific embodiments of the present invention are illustrated in Figures 2, 3 and 4.

~~{The}~~ **[Referring now to Fig. 2, the]** remote controls of set-top box ~~{(STB)}~~ **[32]** and of television set (TV set) **[30]** are combined in one device, control unit (RCU) **[42]**, already in a first integration stage ~~{according to Figure 2}~~. The new control unit ~~{(RCU)}~~ **[42]** receives a smart card interface **[34]**, capable of driving both smart card (ICC DVB) ~~{of}~~ **[38of]** the pay TV system, as well as smart card (ICC BC) **[40]** of the backward channel. In terms of the functional sequence, the key exchange of the conditional access system (CAS) of the pay TV is carried out exactly as in the conventional configuration.

In Figure 2, however, an IR interface **[37]** links smart card ~~{(ICC) DVB}~~ **[38]** via control unit ~~{(RCU)}~~ **[34]** to the pay TV decryption chip **[42]** (e.g., DVB) in set-top box ~~{(STB)}~~ **[32]**. The same applies to smart card ~~{(ICC) BC}~~ **[40]**, which, at this point, likewise safeguards the backward channel via control unit ~~{(RCU)}~~ **[34]** and its IR interface.

It is, therefore, no longer necessary to insert smart cards into set-top box ~~{(STB)}~~ **[32]**, eliminating the need for any smart card interfaces at the set-top box ~~{(STB)}~~ **[32]**. The customer inserts his cards directly into the remote control ~~{RCU}~~ **[34]**. If pay TV providers and backward channel service providers agree contractually to this effect, then the functions of both smart cards ~~{ICC DVB}~~ **[38]** and ~~{ICC BC}~~ **[40]** can even be combined on a single smart card (ICC).

In Figure ~~{2ff,}~~ **[2,]** the computer ~~{PC}~~**[(PC) 41]** either continues to be connected to set-top box ~~{(STB)}~~ **[32]** via a conventional interface (PCI) **[42]** or likewise utilizes the IR interface (infrared interface) **[44]** of set-top box ~~{(STB)}~~ **[32]** for this purpose.

The backward channel connection to the telecommunications network is effected either via set-top box ~~{(STB)}~~ **[32]** or via the computer ~~{(PC)}~~ **[41]**. Both variants are possible in principle.

Figure 3 shows remote control (RCU) and computer (PC) combined in a further integration stage **[into a combined apparatus (RCU/PC) 50]**. Here, one can utilize the advantages of the computer PC and of remote control (RCU) simultaneously. This approach is of particular interest when the combined apparatus ~~{RCU/PC}~~ **[50]** is similar to a "network PC" and can be operated compactly and without complicated peripherals and cabling, e.g., from the ~~{living room}~~ **[coffee]** table.

Figure 4 illustrates the television set (TV set) and set-top box (STB) combined in just one terminal **[70]**, as a further integration stage.

The new terminal configurations illustrated in Figures 2 through 4 show how one can appreciably simplify the operation and cabling of the terminals without degrading functionality.

Therefore, in accordance with the present invention, instead of one or more smart card interfaces on the set-top box (STB), the relevant smart cards are now connected via a remote control ~~{RCU}~~**[(RCU) 76]** and its infrared interfaces **[78]** to the pay TV decryption chip remaining in set-top box ~~{(STB)}~~ **[70]**. Thus, the need is eliminated for costly and delicate interfaces on the set-top box~~{(STB)}~~.

Moreover, the functions of the pay TV smart card and of the backward-channel smart card can be combined in a user-friendly manner on just one card, with the assistance of a special remote control RCU.

Finally, combining the remote control and the PC in ~~{just one}~~ **[combined]** apparatus ~~{RCU/PC}~~ **[76]** makes it possible to move the backward channel connection out of the set-top box ~~{(STB)}~~ **[70]**. This makes it possible to optimally utilize ~~{the}~~ **[an]** internet PC ~~{(=}~~**[(a]** PC which is linked via any desired online networks to servers of any desired service providers), in conjunction with pay TV services, including their backward channel options.

A further aspect of the present invention is configuring the smart card so that it, too, can handle, with a high level of security, both the decryption of the program of the pay TV provider and transactions (ordering and payment of purchase price) with the goods/service provider.

In particular, if further goods/service providers are added over time, this means in each case that the program customer needs a new smart card containing the keys and protocols of the previous providers (both pay TV providers and goods/service providers) and the key and the protocol of the newly added provider.

The present invention likewise provides an approach for this:
Since the goods/service provider is linked in any case, as a rule, to the user by the same host computer as the pay TV provider, this host can also access the inhibited areas of the customer's smart card by a general key, in order to store there a further key and the associated protocol for future transactions (decryption or payment processes).

Moreover, a vector table or an interrogation routine, in which the newly added keys are successively managed, is to be executed in an additional area (possibly likewise inhibited). In response to a smart card access, it is first checked on the basis of the vector table or the interrogation routine to see whether an appropriate key is present, or whether the key input by the user matches one of the keys stored on the smart card. Only when this interrogation has a positive result, is the program associated with the respective key (if indicated, decrypted and then) executed for the purpose of transaction or decryption.

The key and the associated protocol (program) are preferably likewise transmitted in an encrypted form, from the host computer to the **[set-top]** box ~~{(STB)}~~ **[32, 70]** and, from there, routed via the interface to **[the]** control unit ~~{(RCU).}~~ **[34, 50, 76.]** When **[the]** control unit ~~{(RCU)}~~ is integrated ~~{in}~~ **[with]** computer ~~{(PC/RCU)}~~**[(PC) as combined apparatus 50, 76]**, the host computer can be directly linked to **[the]** computer ~~{(PC/RCU)}~~**[(PC)]** via the telecommunications network **[48, 68, 88]**, to transmit the information for ~~{the}~~, ~~{i.e.,}~~ **[or]** into**[,]** smart card ~~{(ICC)}~~ **[38, 40, 72, 74]**.

Depending on the specific configuration, it is possible for the protocol (program) to be stored in the smart card just in an encrypted form, and for it to be decrypted in each case for the delay prior to execution. Alternatively, however, the protocol (program) can also be rendered in an executable form when it is stored in the (protected) memory area of the smart card.

As a result, the memory of the smart card contains (inter alia) the following programs and/or data:

An operating system core for controlling communications between the smart card processor and the peripherals on the smart card, as well as communications with the host computer which manages the memory areas of the smart card (protected and unprotected areas, read/write areas, flash EEPROM, etc.), etc. Keys (a master or general key, and also one or more application keys), the master key being used to transfer (further) application keys and the associated application or protocol programs into the memory area. The application keys ensure that the protocol programs are executed (and thus orders handled or pay TV programs decrypted) only in response to proper user input.

Encrypted user programs or protocol programs for controlling the handling of orders or the decryption of pay TV programs.

To enhance security, provision is made for the identification and authentication between the control unit ~~{(RCU)}~~ **[34, 50, 76]** and/or the set-top box ~~{(STB)}~~ **[32, 70]** or television set ~~{(TV set)}~~ **[30, 70]**, on the one hand, and the host computer, on the other hand, to be carried out on different routes or channels. In other words, some of the protocol traffic is transmitted via interface ~~{(5)}~~ **[5]** to the ~~{telephone}~~ **[telecommunications]** network **[48, 68, 88]**, and some via line ~~{(1)}~~ **[1]**, together with or prior to the broadband, digitally encrypted pay TV useful signal. In this context, the enabling/inhibiting of services can also take place on these routes. Since a case of misuse would require synchronously intercepting and decrypting both channels, security is thus considerably higher. In particular, information can be distributed between the two channels at the time of enabling/inhibiting, or of new keys, etc., in such a way that it is able to be decrypted only in an alternating and also only in a step-by-step manner, in each instance, with knowledge thereof.

[2345/115]

DECODER DEVICE FOR DECRYPTING ENCRYPTED TELEVISION PROGRAMS

The invention relates to a decoder device for decrypting encrypted television programs. In particular, the present invention relates to a decoder device having a control unit, for the decryption of encrypted television programs, having an input for feeding in an encrypted television program, a decryption device, which decrypts an encrypted television program into a format that can be reproduced by a television receiver, an output, which can be connected to a television receiver in order to feed the decrypted television program into the television receiver for reproduction, an interface for an identification and/or key carrier component for enabling the decryption device, and an interface for a control unit of the decoder device.

A decoder device of this type enables the reception and decryption of so-called pay TV programs, present-day decoder devices being commercially available as so-called set-top boxes for conventional television receivers.

The invoicing that has been customary heretofore, for example monthly invoicing, for supplying programs in pay TV is shifting more and more to an individual ("pay-per-view") invoicing practice. Therefore, there is a need to identify and authenticate the program customer before the program customer accesses the program. In addition, in the case of so-called HOT programs (home order television), the program customer's orders are also debited to said customer's bank account or his credit on a smart card. Here, too, it is necessary to identify and authenticate the program customer and, when needed, implement security mechanisms to protect against misuse.

To secure electronic invoicing processes, and to protect confidential information (bank account data, account balances, etc.), use is made of smart cards having microprocessors which are equipped with encryption algorithms. An encryption algorithm of this type is the so-called RSA algorithm. In the case of pay TV, a smart card of this type is part of the so-called "conditional access system" (CAS), which is used to check whether the person making the inquiry is actually the authorized program customer and, if applicable, whether his creditworthiness suffices for the desired service. In so-called "electronic commerce", as well, this smart card represents the identity of the customer or of his electronic purse. In this context, a replenishable credit can be recorded on the smart card. The smart card is generally accessed, in a more or less automated manner, by third parties (program providers, commercial entities or the like), via telephone or the internet, using the set-top box before or during the transaction.

A growing problem in this connection is the rising number of program or service providers which a program customer can subscribe to via these media. The result is an ever increasing outlay for equipment (set-top box, television set, internet terminal (PC or net PC), remote control units for the set-top box and the television set, as well as an ever increasing number of smart cards needed to utilize the individual services.

The object of the present invention is, therefore, to design these various components to be less expensive, i.e., to reduce their hardware outlay, and to design them to be less susceptible to faults and simpler for the program customer to handle. Moreover, the present invention intends to consider the problem of security

which is becoming increasingly relevant, in connection with services being utilized by unauthorized third parties.

This objective is achieved in accordance with the present invention by configuring the interface for the identification and/or key carrier component in the control unit of the decoder device.

This design makes it possible to reduce the number of interfaces. Moreover, the program customer (user) is able to carry out his transactions in a more convenient manner, since the control unit of the decoder device is equipped with a keypad in any case. Furthermore, security is improved, since the program customer (even among a relatively large number of third parties) can effect his inputs (PIN, TAN, etc.) without third parties being able to observe this. Moreover, the control unit of the decoder device can be kept securely, together with the identification and/or key carrier component, (smart card), whereas, as a rule, for the sake of convenience, a smart card is not removed from the decoder device (= set-top box).

In accordance with one preferred embodiment of the decoder device having a control unit in accordance with the present invention, the control unit is also set up for controlling the television receiver set, which has an interface for receiving control commands from the control unit. This constitutes a further reduction in equipment outlay. Moreover, overall access to the television receiver set can be controlled. In other words, even television use for programs that do not involve payment must be enabled by the authorized user. This can be achieved by having the function of the control unit as a

whole depend on the authorized user inputting the identifier (PIN).

In order for the program provider to handle debiting and to identify the program customer, in the case of the decoder device according to the present invention, use is made, in particular, of an interface to a telecommunications network. This can be a modem, or a corresponding coupling device for digital telecommunications networks.

In particular, to enhance security in the system, an interface to an identification and/or key carrier component is used. Via such an interface to a telecommunications network, the program customer can make contact with a service provider or merchandise shipper. Here as well, a connection to a specific subscriber (service provider or merchandise shipper) via the telecommunications network is established as a function of an authorization by the identification and/or key carrier component. The program provider is thus considered independently of the service provider or merchandise shipper, when the program customer is invoiced. This can be advantageous with respect to data security and flexibility.

Alternatively, however, it is also possible that the program provider and the service provider cooperate in a suitable fashion, making it possible to have a shared invoicing and/or customer administration, as well as customer identification and customer authorization. In such a case, there is no need for separate smart cards.

At any rate, it is advantageous for the interface to the identification and/or key carrier component for the

authorization of the connection via the telecommunications network to also be arranged in the control unit.

As already mentioned, the identification and/or key carrier component for the authorization of the connection via the telecommunications network and the identification and/or key carrier component for enabling the decryption device can be implemented either by two separate or by one common smart card.

In a further refinement, the decoder device is provided with an interface for connecting the decoder device to a computer, which is set up for controlling the decoder device and/or for establishing a connection to another subscriber via the telecommunications network. It is, thus, possible to make available to the program customer the entire functionality of a computer (PC or internet PC), i.e., the storing and processing of data and information, as well as the more convenient configuration of dialogs between the program customer and, for example, the program provider or the service provider.

In one especially preferred specific embodiment of the present invention, the control unit is formed by the computer, which has an interface for controlling the decoder device, and an interface for the identification and/or key carrier component for authorizing the connection via the telecommunications network and/or the identification and/or key carrier component for enabling the decryption device. This eliminates the need for one or two separate control units. It goes without saying that in this specific embodiment as well, the two smart cards for the traffic with the program provider and the service provider can also be realized as one common smart

card.

It should also be mentioned that the connection between the computer and the television set, or the computer and the decoder device, can either be wire-free (for example, an infrared or ultrasonic connection) or wire-based. In addition, the special demands placed on the computer (relatively small memory, no need for an especially ergonomic keyboard due to mostly short inputs, etc.), mean that a so-called palmtop design is possible, with the appropriate interfaces (infrared interface to the decoding device of one such or more interfaces for the smart card(s)). Thus, the user is able to control and operate his equipment in a very compact and convenient manner, and also simply and conveniently communicate with the program provider and/or the service/merchandise provider. Finally, there is also a substantial reduction in the outlay for cabling between the individual components at the user end, which likewise enhances the convenience.

One especially preferred specific embodiment of the present invention provides for the decoder device to be integrated in the television set. The user is thus provided with a self-contained apparatus which is specially protected against misuse, and in which all of the functions (conventional television, pay TV, communication with a service/merchandise provider via the telecommunications network, storage and/or post-processing of the received data in the computer, etc.) can be performed in a manner in which they are protected from misuse.

The present invention also relates to a smart card for an above-described decoder device with a control unit,

having a computer unit, a first memory area, in which are stored at least parts of operating system functions which are used to control the communication between the computer unit of the smart card and the peripherals of the smart card, as well as the communication with an external host computer, and which are used to manage protected, unprotected and/or read/write memory areas of the smart card, and having a second memory area, which is subdivided into protected and unprotected areas, access to protected areas being made as a function of a check for permitted access, a general key being stored in the protected area of the second memory area, and under the control of the general key, the external host computer entering at least one further simple key, as well as a protocol program associated with this further simple key.

This smart card makes it possible for the decoder device described above to be operated quite securely and also simply, thereby expanding the access to a plurality of additional service providers.

Preferably stored in the second memory area is a key management, from which access is made to a protocol program of a simple key.

In this context, the following method according to the present invention is used to supplement additional keys, i.e., ways of accessing additional providers:

- a telecommunications connection is established by the host computer between the host computer and the decoder device with the control unit or the computer containing the control unit;
- the host computer checks the general key in the smart card;
- a simple key, as well as a protocol program

associated with the key are communicated to the smart card in encrypted form, in the case that the check test has a positive result;

- the simple key and the protocol program associated with the key are entered into the protected memory area of the smart card;
- the protected memory area of the smart card is inhibited.

In this context, before the simple key and the protocol program associated with the key are entered into the protected memory area of the smart card, the key and the protocol program can be decrypted by the computer unit of the smart card.

Figure 1 shows a related-art arrangement in a schematic block diagram.

Figures 2 - 4 depict various specific embodiments of the present invention, each in a schematic block diagram.

Figure 1 illustrates terminal environment for combined pay TV and electronic commerce applications that is customary today. The broadband, digitally encrypted pay TV useful signal is received by the television set via line (1) and transferred via output (4) to input (IN), into set-top box (STB). There, the signal is decrypted by a special chip using an algorithm provided for this - the DVB algorithm is mentioned here as being representative of all such algorithms - and retransmitted to the television set. The keys are set by a smart card (ICC DVB) via interface (3). The smart card contains the key-distribution algorithm of the conditional access system (e.g. RSA) and the customer's secret key. Only a customer having a valid smart card (ICC DVR) is able to decrypt

pay TV broadcasts. The smart card (ICC DVR) is connected to set-top box (STB) via smart card interface "IFD".

Enhancements to set-top box (STB) envisage connecting a backward channel via the telephone network or internet via interface (5) to the servers of various service providers, e.g., for ordering services or goods advertised on the pay TV channels. To safeguard the order and payment, a second smart card (ICC BC) can be inserted in this case via a further interface (IFD), establishing connection (6) between second smart card (ICC BC) and second interface (IFD).

Other possible enhancements for linking set-top box (STB) envisage using an IR remote control (9) and a computer PC via an interface (7) that is customary in the PC environment, referred to here simply as "PCI" (e.g., V24/RS232C or parallel interface). The computer PC facilitates, for example, user-friendly backward channel transactions or the post-processing of information from the pay TV channels.

There are various ways to connect two smart cards to set-top box (STB). Either smart card terminals (IFD) are permanently installed in set-top box (STB), or they are designed to be insertable as PCMCIA modules. PCMCIA modules make it possible to exchange one pay TV access method (CAS) for another without any intervention in set-top box (STB).

Disadvantages associated with conventional terminal configurations include the lack of user-friendliness, the elaborate cabling of set-top box (STB), and its complicated interface configuration.

Specific embodiments of the present invention are illustrated in Figures 2, 3 and 4.

The remote controls of set-top box (STB) and of television set (TV set) are combined in one device, control unit (RCU), already in a first integration stage according to Figure 2. The new control unit (RCU) receives a smart card interface, capable of driving both smart card (ICC DVB) of the pay TV system, as well as smart card (ICC BC) of the backward channel. In terms of the functional sequence, the key exchange of the conditional access system (CAS) of the pay TV is carried out exactly as in the conventional configuration.

In Figure 2, however, an IR interface links smart card (ICC) DVB via control unit (RCU) to the pay TV decryption chip (e.g., DVB) in set-top box (STB). The same applies to smart card (ICC) BC, which, at this point, likewise safeguards the backward channel via control unit (RCU) and its IR interface.

It is, therefore, no longer necessary to insert smart cards into set-top box (STB), eliminating the need for any smart card interfaces at the set-top box (STB). The customer inserts his cards directly into the remote control RCU. If pay TV providers and backward channel service providers agree contractually to this effect, then the functions of both smart cards ICC DVB and ICC BC can even be combined on a single smart card (ICC).

In Figure 2ff, the computer PC either continues to be connected to set-top box (STB) via a conventional interface (PCI) or likewise utilizes the IR interface (infrared interface) of set-top box (STB) for this purpose.

The backward channel connection to the telecommunications network is effected either via set-top box (STB) or via the computer (PC). Both variants are possible in principle.

Figure 3 shows remote control (RCU) and computer (PC) combined in a further integration stage. Here, one can utilize the advantages of the computer PC and of remote control (RCU) simultaneously. This approach is of particular interest when the combined apparatus RCU/PC is similar to a "network PC" and can be operated compactly and without complicated peripherals and cabling, e.g., from the living room table.

Figure 4 illustrates the television set (TV set) and set-top box (STB) combined in just one terminal, as a further integration stage.

The new terminal configurations illustrated in Figures 2 through 4 show how one can appreciably simplify the operation and cabling of the terminals without degrading functionality.

Therefore, in accordance with the present invention, instead of one or more smart card interfaces on the set-top box (STB), the relevant smart cards are now connected via a remote control RCU and its infrared interfaces to the pay TV decryption chip remaining in set-top box (STB). Thus, the need is eliminated for costly and delicate interfaces on the set-top box (STB).

Moreover, the functions of the pay TV smart card and of the backward-channel smart card can be combined in a user-friendly manner on just one card, with the assistance of a special remote control RCU.

Finally, combining the remote control and the PC in just one apparatus RCU/PC makes it possible to move the backward channel connection out of the set-top box (STB). This makes it possible to optimally utilize the internet PC (= PC which is linked via any desired online networks to servers of any desired service providers), in conjunction with pay TV services, including their backward channel options.

A further aspect of the present invention is configuring the smart card so that it, too, can handle, with a high level of security, both the decryption of the program of the pay TV provider and transactions (ordering and payment of purchase price) with the goods/service provider.

In particular, if further goods/service providers are added over time, this means in each case that the program customer needs a new smart card containing the keys and protocols of the previous providers (both pay TV providers and goods/service providers) and the key and the protocol of the newly added provider.

The present invention likewise provides an approach for this:
Since the goods/service provider is linked in any case, as a rule, to the user by the same host computer as the pay TV provider, this host can also access the inhibited areas of the customer's smart card by a general key, in order to store there a further key and the associated protocol for future transactions (decryption or payment processes).

Moreover, a vector table or an interrogation routine, in which the newly added keys are successively managed, is

to be executed in an additional area (possibly likewise inhibited). In response to a smart card access, it is first checked on the basis of the vector table or the interrogation routine to see whether an appropriate key is present, or whether the key input by the user matches one of the keys stored on the smart card. Only when this interrogation has a positive result, is the program associated with the respective key (if indicated, decrypted and then) executed for the purpose of transaction or decryption.

The key and the associated protocol (program) are preferably likewise transmitted in an encrypted form, from the host computer to the box (STB) and, from there, routed via the interface to control unit (RCU). When control unit (RCU) is integrated in computer (PC/RCU), the host computer can be directly linked to computer (PC/RCU) via the telecommunications network, to transmit the information for the, i.e., into smart card (ICC).

Depending on the specific configuration, it is possible for the protocol (program) to be stored in the smart card just in an encrypted form, and for it to be decrypted in each case for the delay prior to execution. Alternatively, however, the protocol (program) can also be rendered in an executable form when it is stored in the (protected) memory area of the smart card.

As a result, the memory of the smart card contains (inter alia) the following programs and/or data:

An operating system core for controlling communications between the smart card processor and the peripherals on the smart card, as well as communications with the host computer which manages the memory areas of the smart card

(protected and unprotected areas, read/write areas, flash EEPROM, etc.), etc. Keys (a master or general key, and also one or more application keys), the master key being used to transfer (further) application keys and the associated application or protocol programs into the memory area. The application keys ensure that the protocol programs are executed (and thus orders handled or pay TV programs decrypted) only in response to proper user input.

Encrypted user programs or protocol programs for controlling the handling of orders or the decryption of pay TV programs.

To enhance security, provision is made for the identification and authentication between the control unit (RCU) and/or the set-top box (STB) or television set (TV set), on the one hand, and the host computer, on the other hand, to be carried out on different routes or channels. In other words, some of the protocol traffic is transmitted via interface (5) to the telephone network, and some via line (1), together with or prior to the broadband, digitally encrypted pay TV useful signal. In this context, the enabling/inhibiting of services can also take place on these routes. Since a case of misuse would require synchronously intercepting and decrypting both channels, security is thus considerably higher. In particular, information can be distributed between the two channels at the time of enabling/inhibiting, or of new keys, etc., in such a way that it is able to be decrypted only in an alternating and also only in a step-by-step manner, in each instance, with knowledge thereof.

Revised Claims

1. A decoder device (STB) having a control unit (RCU) for decrypting encrypted television programs, comprising
- an input (4) for feeding in an encrypted television program;
- a decryption device (DVB), which decrypts an encrypted television program into a format that can be reproduced by a television set (TV);
- an output (2), which can be connected to a television set (TV) in order to feed the decrypted television program into the television set (TV) for reproduction;
- an interface (IFD 3,6) for an identification and/or key carrier component (ICC DVB) for enabling the decryption device (DVB); and
- an interface (IR 3,6) for a control unit (RCU) of the decoder device (STB); and
- an interface (BC 5) to a telecommunications network (tel. network);
characterized in that
- the interface (IFD 3,6) for the identification and/or key carrier component (ICC DVB) is arranged in the control unit (RCU) of the decoder device (STB); and
- an interface (IFD 3,6) to an identification and/or key carrier component (ICC BC) is present, a connection being established via the telecommunications network (tel. network) to a specific subscriber as a function of an authorization by the identification and/or key carrier component (ICC BC).

2. The decoder device having a control unit (RCU) as recited in Claim 1, characterized in that
- the interface (IFD 3,6) to the identification and/or key carrier component (ICC BC) for authorizing the

connection via the telecommunications network (tel. network) is arranged in the control unit (RCU).

3. The decoder device (STB) having a control unit (RCU) as recited in Claim 1 or 2, characterized in that

- the control unit (RCU) is also set up for controlling the television receiver (TV set), which has an interface (IR 9) for receiving control commands.

4. The decoder device (STB) having a control unit (RCU) as recited in one of the preceding claims, characterized in that

- the identification and/or key carrier component (ICC BC) for authorizing the connection via the telecommunications network (tel. network) and the identification and/or key carrier component (ICC BVB) for enabling the encryption device (DVB) are implemented either by two separate or by one common smart card.

5. The decoder device (STB) having a control unit (RCU) as recited in one of the preceding claims, characterized in that

- the decoder device (STB) has an interface (PCI) via which the decoder device (STB) can be connected to a computer (PC), which is set up for controlling the decoder device (STB) and/or for establishing a connection to another subscriber via the telecommunications network (tel. network).

6. The decoder device (STB) having a control unit (RCU) as recited in one of the preceding claims, characterized in that

- the control unit (RCU) is made up of the computer (PC), which
- has an interface (IR 3,6,7) for controlling the decoder device (STB); and
- an interface (IFD 3,6) for the identification and/or

key carrier component (ICC BC) for authorizing the connection via the telecommunications network (tel. network) and/or the identification and/or key carrier component (ICC DVB) for enabling the decryption device (DVB).

7. The decoder device (STB) having a control unit (RCU) as recited in one of the preceding claims, characterized in that

- the decoder device (STB) is integrated in the television set (TV).

8. A smart card for a decoder device having a control unit (RCU) as recited in one of the preceding claims, comprising

- a computer unit;
- a first memory area, in which are stored at least parts of operating system functions which are used to control the communication between the computer unit of the smart card and the peripherals of the smart card, as well as the communication with an external host computer, and which are used to manage protected, unprotected and/or read/write memory areas of the smart card;

and

- a second memory area, which is subdivided into protected and unprotected areas, access to protected areas being made as a function of a check for permitted access,

characterized in that

- a general key is stored in the protected area of the second memory area, and under the control of the general key, the external host computer enters at least one further simple key, as well as a protocol program associated with this further simple key.

9. The smart card as recited in Claim 10, characterized

in that

- stored in the second memory area is a key management, from which access is made to a protocol program of a simple key.

10. A method for a host computer of a pay TV provider to communicate with a decoder device having a control unit (RCU) as recited in one of Claims 1 - 7, and a smart card according to Claim 8 or 9, characterized by the following steps:

- a telecommunications connection is established by the host computer between the host computer and the decoder device with the control unit or the computer containing the control unit;
- the host computer checks the general key in the smart card;
- a simple key, as well as a protocol program associated with the key are communicated to the smart card in encrypted form, in the case that the check test has a positive result;
- the simple key and the protocol program associated with the key are entered into the protected memory area of the smart card;
- the protected memory area of the smart card is inhibited.

11. The method as recited in Claim 10, characterized in that

- before the simple key and the protocol program associated with the key are entered into the protected memory area of the smart card, the key and the protocol program are decrypted by the computer unit of the smart card.

12. The method as recited in Claim 10, characterized in that some of the data transmission traffic is transmitted

back and forth via the interface (5) to the telephone network, and some via a line (1), which is linked to the television set (TV) for transmitting the encrypted television program, together with or prior to a useful signal that reproduces the encrypted television program, the information to be transmitted being distributed and transmitted in such a way that it is able to be decrypted only in an alternating and also only in a step-by-step manner, in each instance, with knowledge thereof.

Abstract

A decoder device having a control unit for decrypting encrypted television programs, including an input for feeding in an encrypted television program, a decryption device, which decrypts an encrypted television program into a format that can be reproduced by a television receiver, an output, which can be connected to a television receiver in order to feed the decrypted television program into the television receiver for reproduction, an interface for an identification and/or key carrier component for enabling the decryption device (DVB), and an interface for a control unit of the decoder device, the interface for the identification and/or key carrier component being arranged in the control unit of the decoder device.

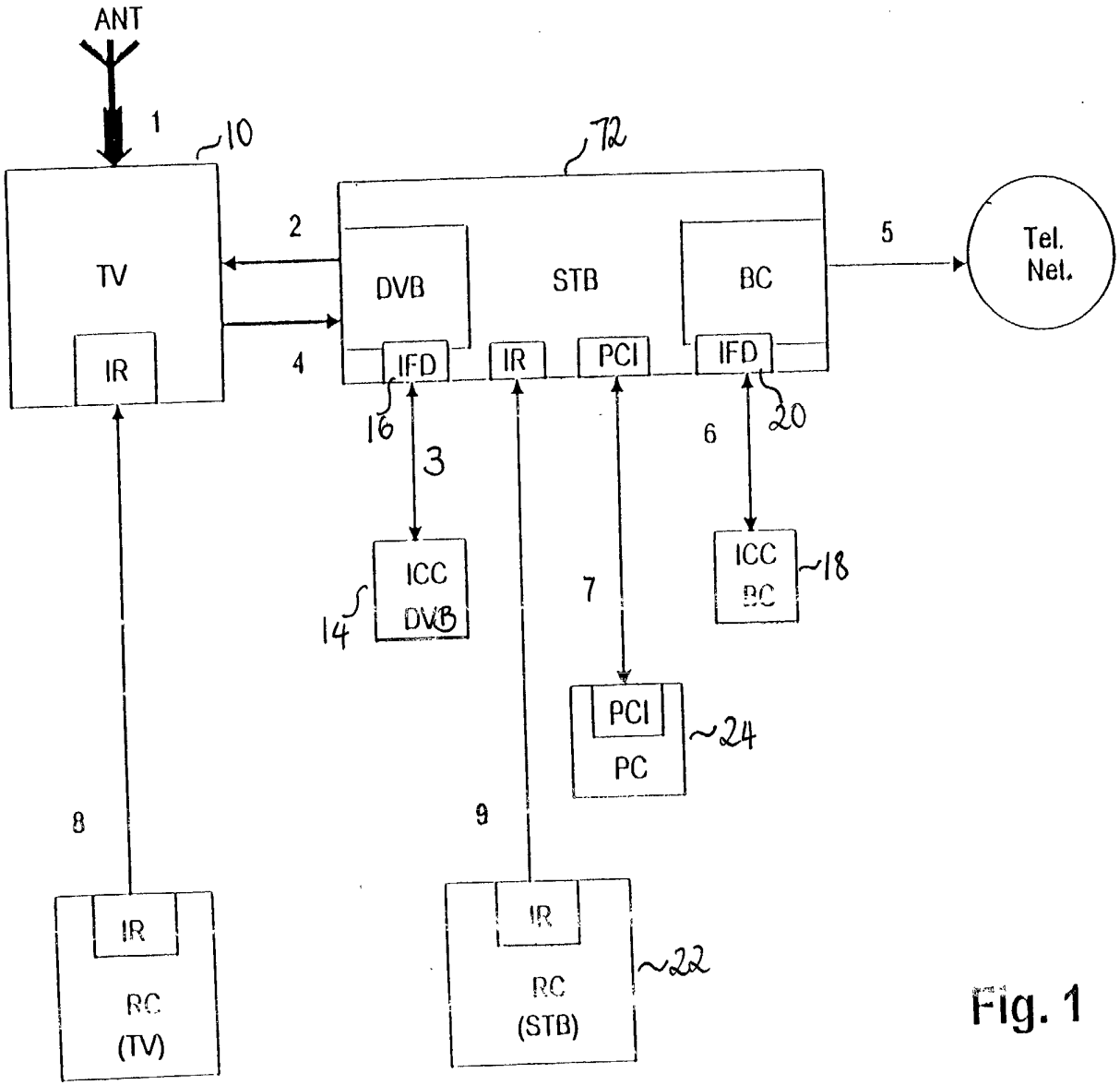

Fig. 1

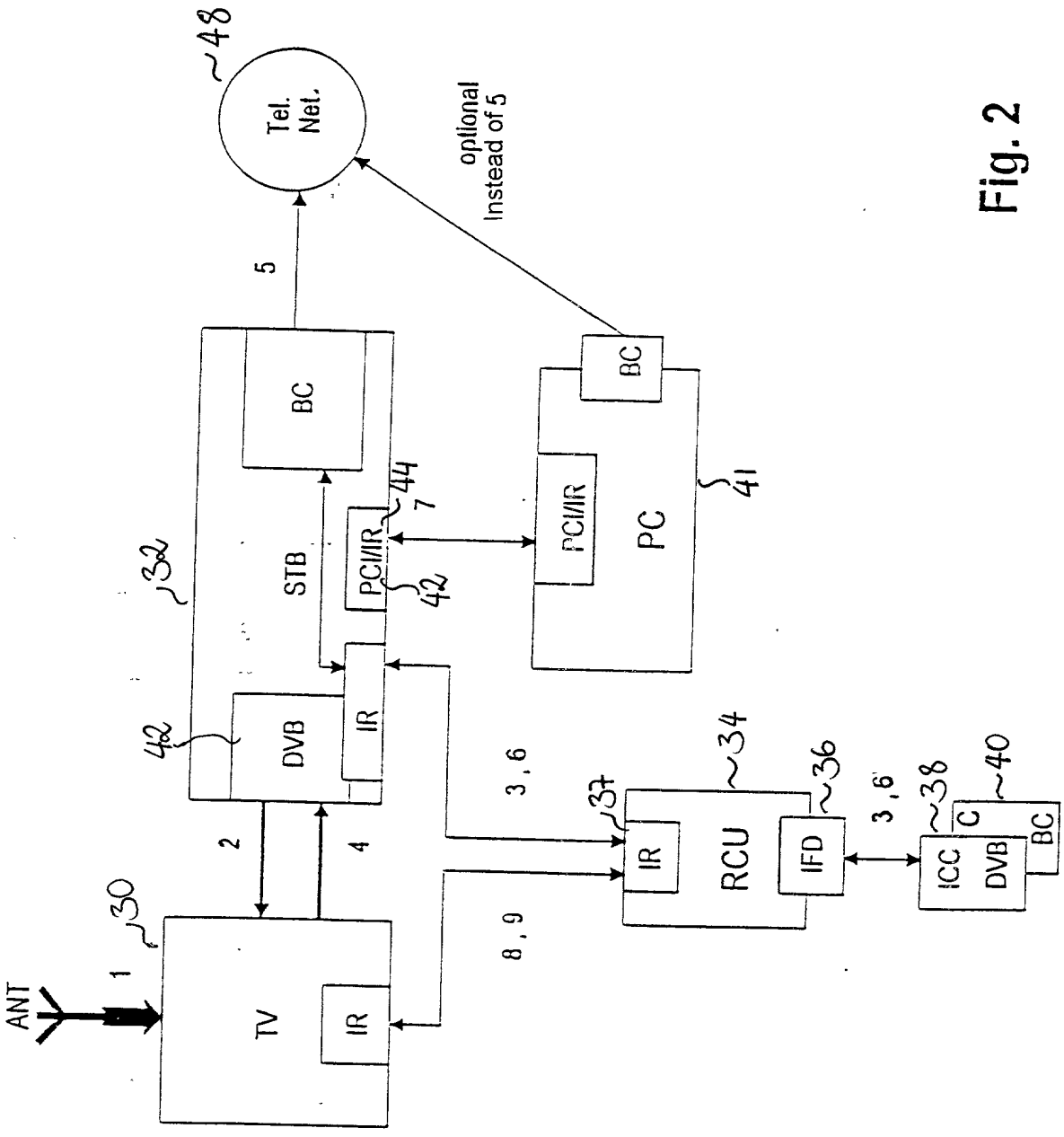
ANT
1
30
TV
IR
2
4
32
42
DVB
IR
STB
BC
5
48
Tel.
Net.
optional
Instead of 5
PCI/IR
44
7
42
PCI/IR
PC
BC
41
3, 6
8, 9
37
IR
RCU
34
IFD
36
3, 6'
ICC
C
38
DVB
BC
40

Fig. 2

09/485408

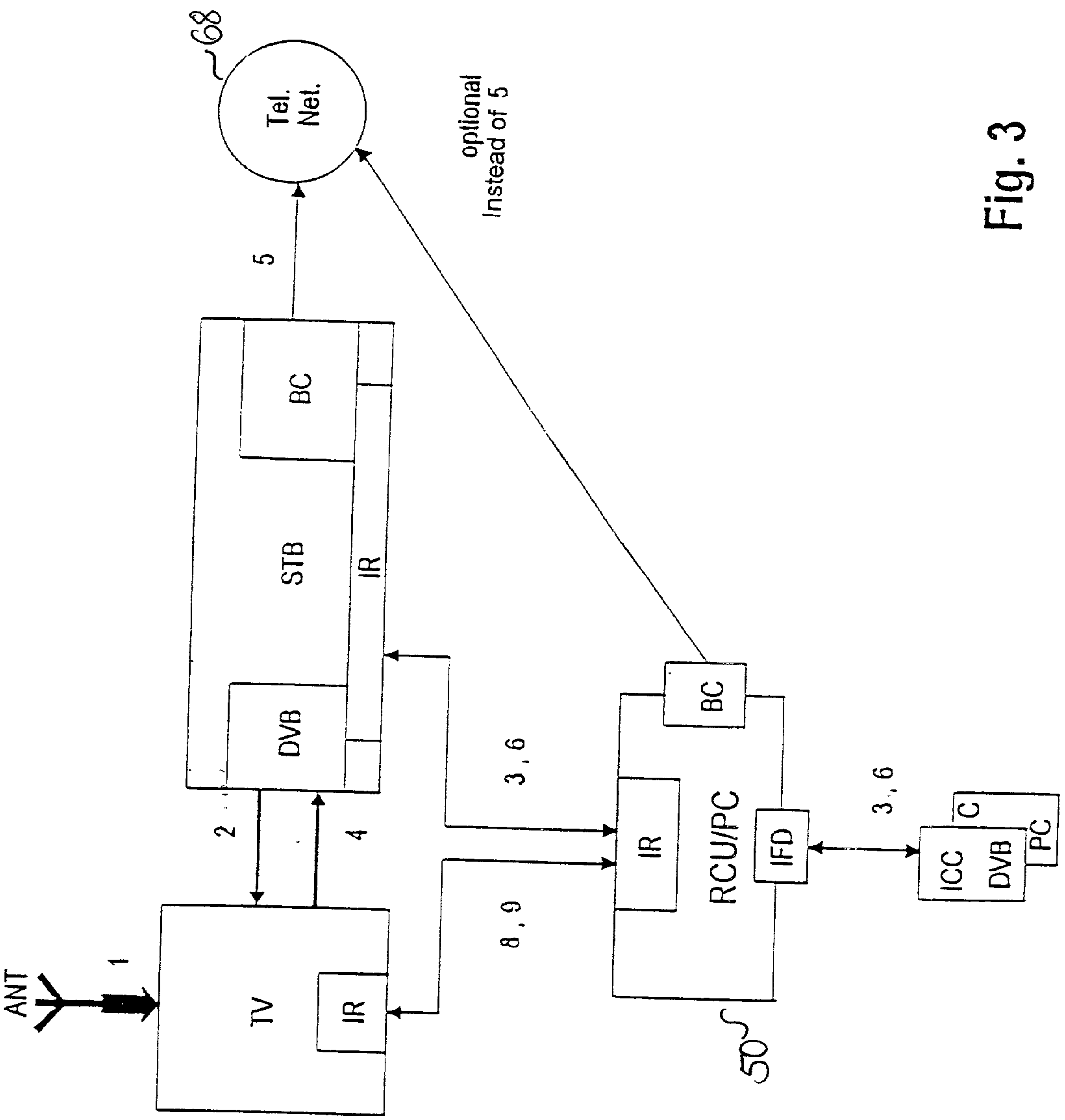

Fig. 3

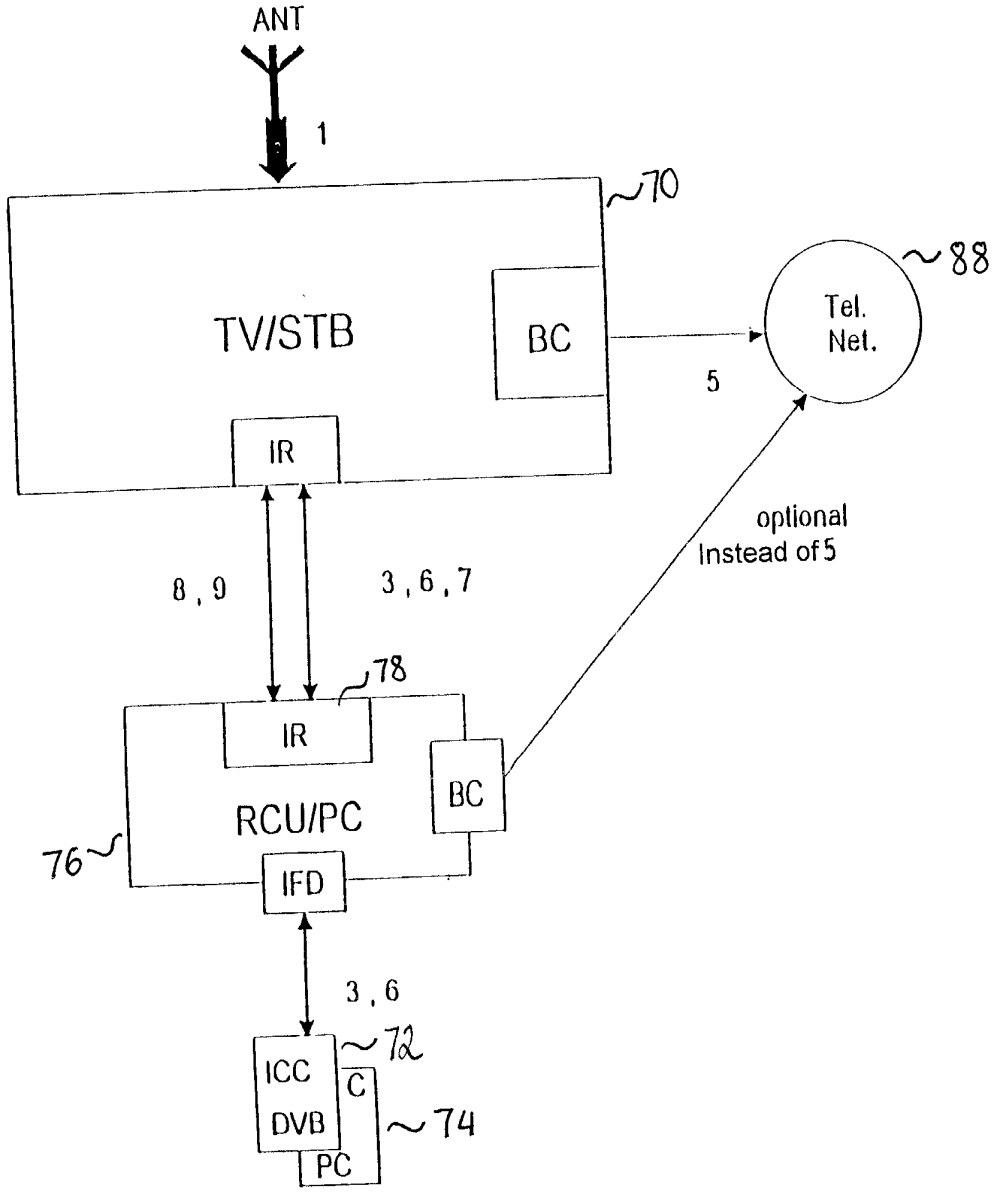

Fig. 4

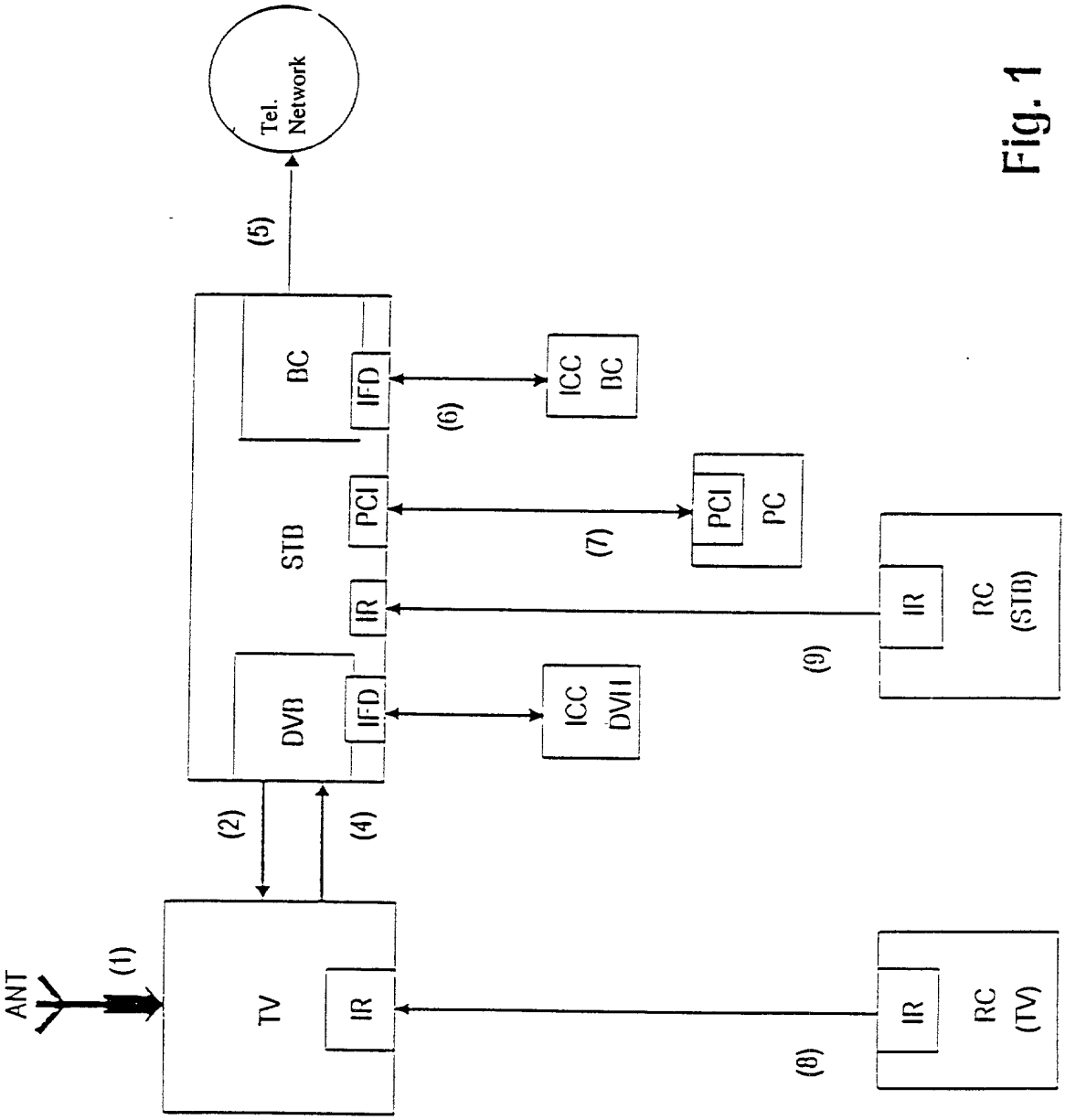
ANT
(1)
TV
IR
(2)
(4)
STB
DVB
IFD
BC
IFD
PCI
IR
(5)
Tel. Network
(6)
ICC BC
(7)
PCI
PC
ICC DVII
(8)
IR
RC (TV)
(9)
IR
RC (STB)

Fig. 1

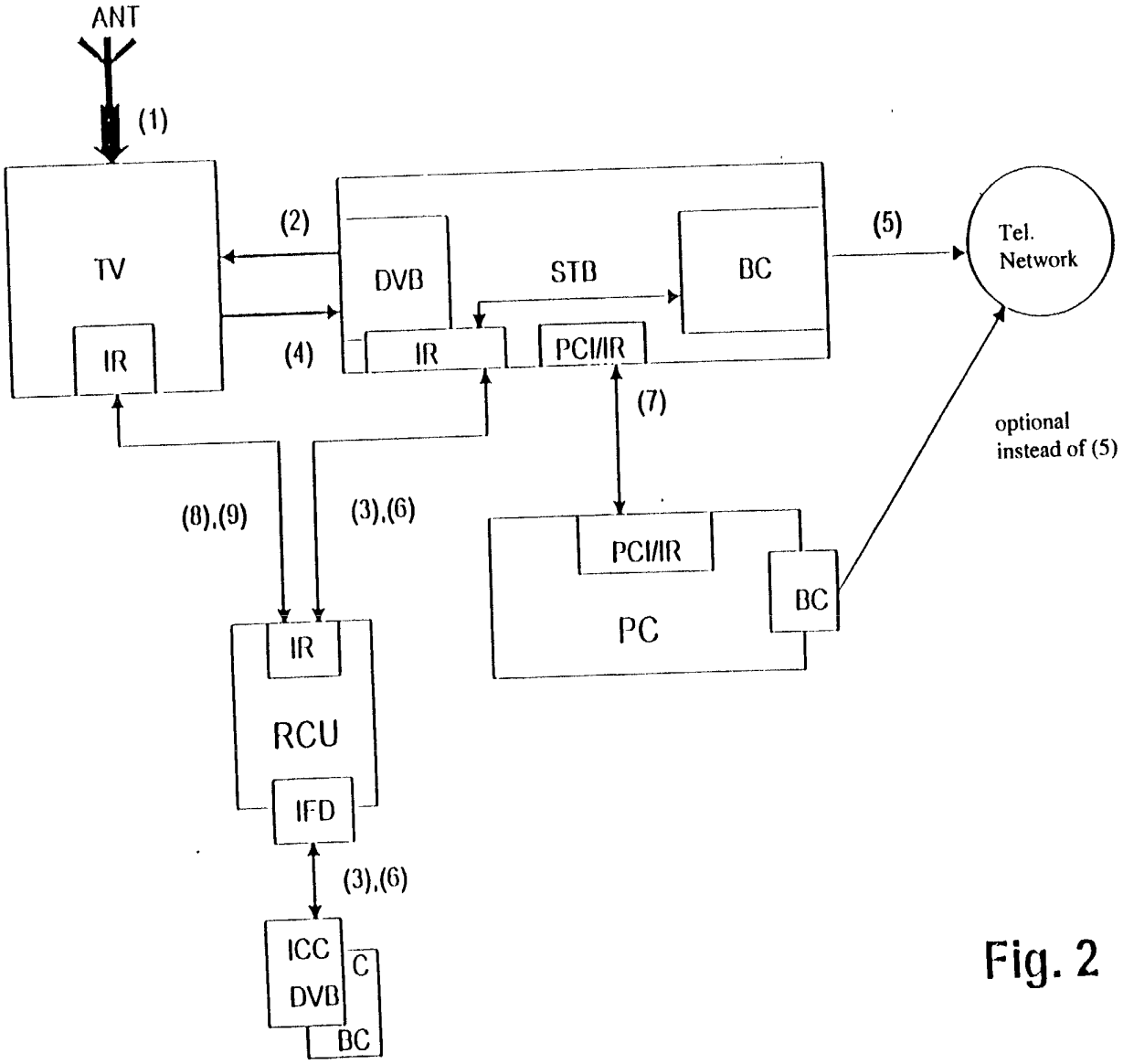

Fig. 2

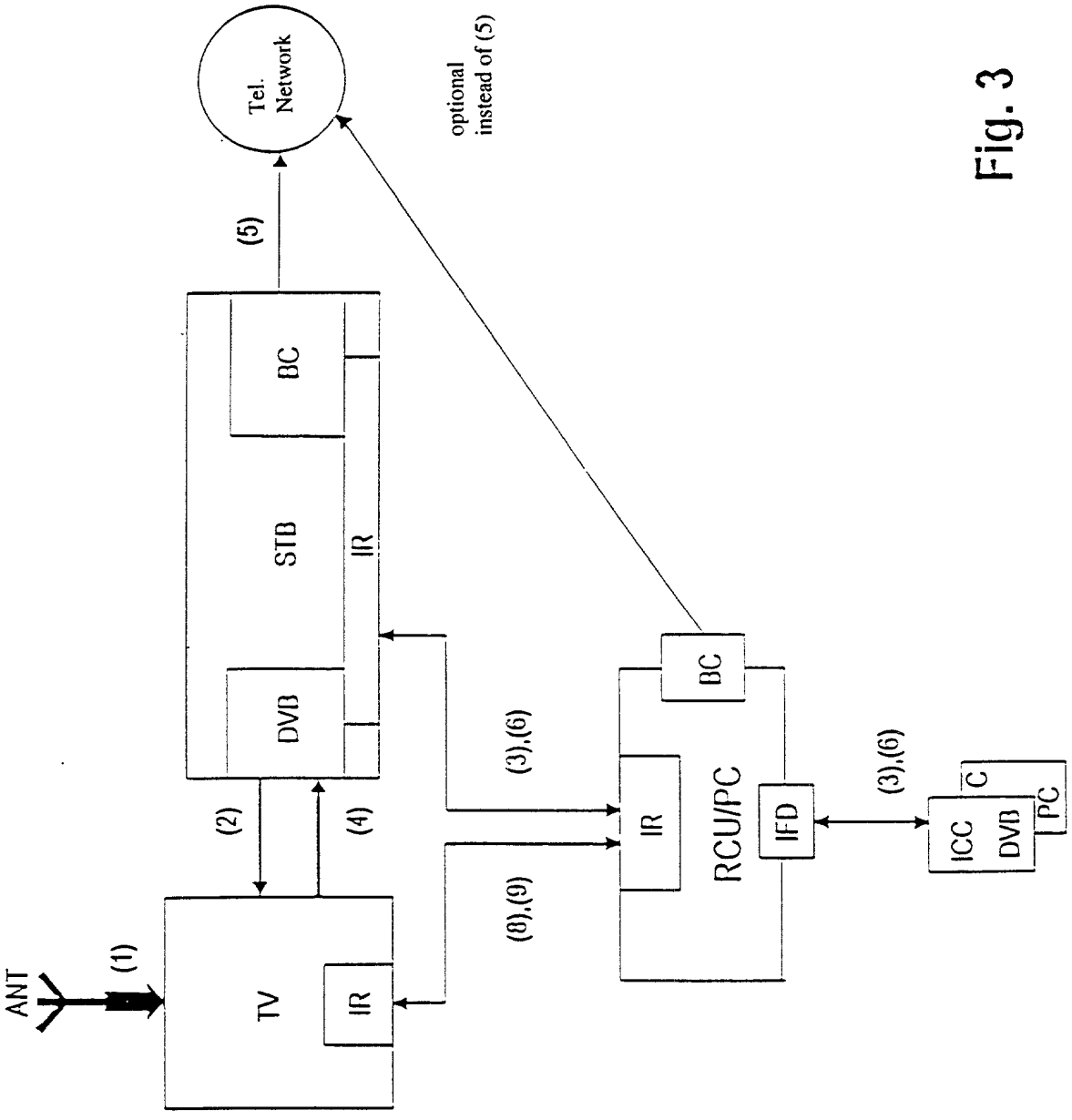
ANT
(1)
TV
IR
(2)
(4)
STB
DVB
IR
BC
(5)
Tel. Network
optional instead of (5)
(3),(6)
(8),(9)
IR
RCU/PC
IFD
BC
(3),(6)
ICC
DVB
C
PC

Fig. 3

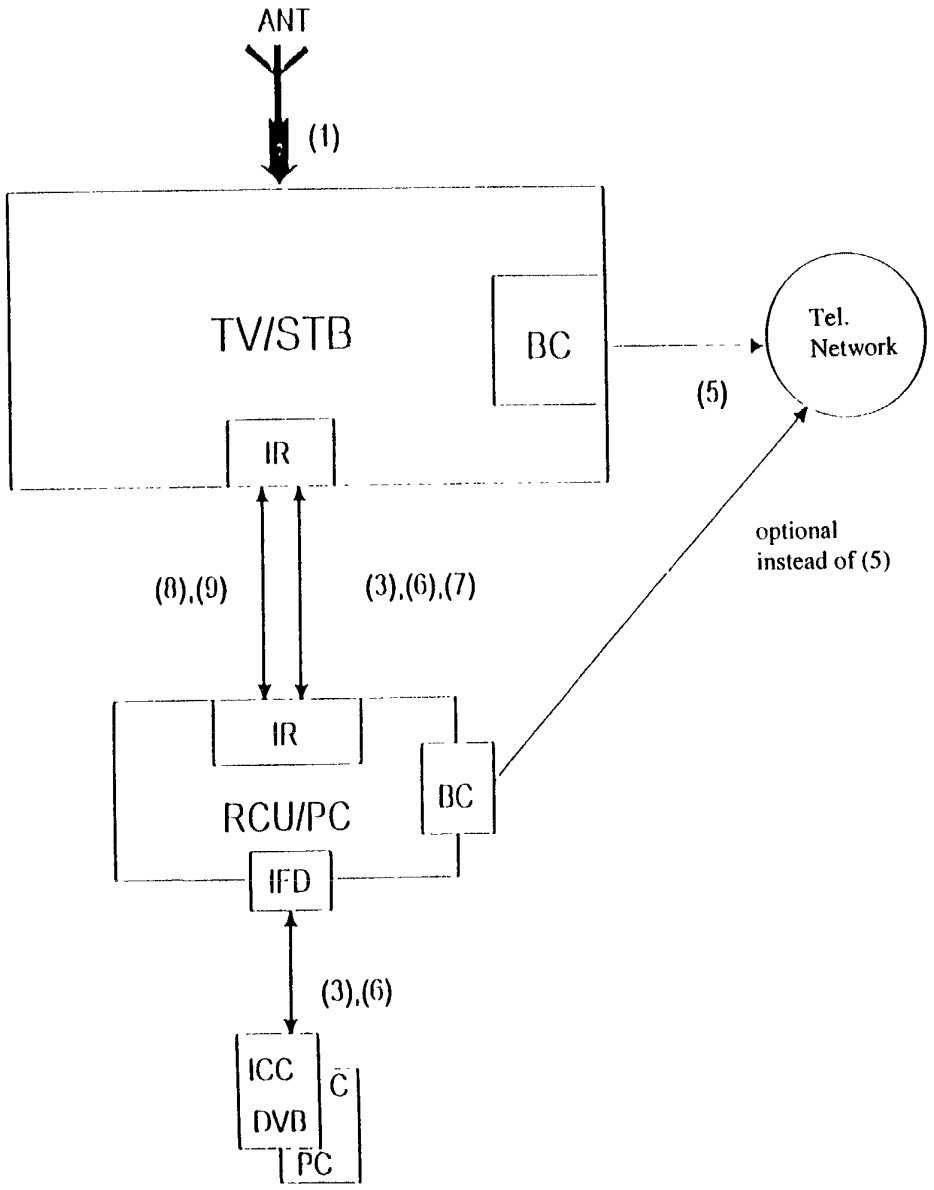
ANT
(1)
TV/STB
BC
Tel.
Network
(5)
IR
optional
instead of (5)
(8),(9)
(3),(6),(7)
IR
RCU/PC
BC
IFD
(3),(6)
ICC
DVB
C
PC

Fig. 4

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	
DECLARATION AND POWER OF ATTORNEY	ATTORNEY'S DOCKET NO. **2345/115**

As a below named inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name,

I believe I am an original, first, and joint inventor of the subject matter that is claimed and for which a patent is sought on the invention entitled **TRANSCODER FOR DECODING ENCODED TV PROGRAMS**, the specification of which was filed as International Application No. PCT/EP98/04424 on July 16, 1998, and is filed herewith in the United States Patent and Trademark Office.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

PRIOR FOREIGN APPLICATION(S)

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

COUNTRY	APPLICATION NUMBER	DATE OF FILING (day, month, year)	DATE OF ISSUE (day, month, year)	PRIORITY CLAIMED UNDER 35 U.S.C. § 119
GERMANY	**197 34 071.7** ✓	**6 August 1997** ✓		**YES**

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorneys:
Richard L. Mayer (Reg. No. 22,490)
Erik R. Swanson (Reg. No. 40,833)

SEND CORRESPONDENCE, AND DIRECT TELEPHONE CALLS TO:

Richard L. Mayer
KENYON & KENYON
One Broadway
New York, New York 10004
(212) 425-7200 (phone)
(212) 425-5288 (facsimile)

EL179105317

I declare that all statements made herein of my own knowledge are true and all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under § 1001 of Title 18 of the United States Code and that such willful statements may jeopardize the validity of the application or any patent issuing thereon.

1-00

FULL NAME OF INVENTOR	FAMILY NAME **WILHELM**	FIRST GIVEN NAME **Siegfried**	SECOND GIVEN NAME
RESIDENCE & CITIZENSHIP	CITY & ZIP CODE **D-81373 Muenchen**	STATE & OR FOREIGN COUNTRY **Germany** OEX	COUNTRY OF CITIZENSHIP **Germany**
POST OFFICE ADDRESS	POST OFFICE ADDRESS **Spitzwegstrasse 4**	CITY & ZIP CODE **D-81373 Muenchen**	STATE OR FOREIGN COUNTRY **Germany**
Signature	X Siegf. E. Wilhelm	Date	02/02/00
FULL NAME OF INVENTOR	FAMILY NAME **KOWALSKI**	FIRST GIVEN NAME **Bernd**	SECOND GIVEN NAME
RESIDENCE & CITIZENSHIP	CITY & ZIP CODE **D-57072 Siegen**	STATE & OR FOREIGN COUNTRY **Germany**	COUNTRY OF CITIZENSHIP **Germany**
POST OFFICE ADDRESS	POST OFFICE ADDRESS **Am Bastenberg 4**	CITY & ZIP CODE **D-57072 Siegen**	STATE OR FOREIGN COUNTRY **Germany**
Signature		Date	

I declare that all statements made herein of my own knowledge are true and all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under § 1001 of Title 18 of the United States Code and that such willful statements may jeopardize the validity of the application or any patent issuing thereon.

FULL NAME OF INVENTOR	FAMILY NAME **WILHELM**	FIRST GIVEN NAME **Siegfried**	SECOND GIVEN NAME
RESIDENCE & CITIZENSHIP	CITY & ZIP CODE **D-81373 Muenchen**	STATE & OR FOREIGN COUNTRY **Germany**	COUNTRY OF CITIZENSHIP **Germany**
POST OFFICE ADDRESS	POST OFFICE ADDRESS **Spitzwegstrasse 4**	CITY & ZIP CODE **D-81373 Muenchen**	STATE OR FOREIGN COUNTRY **Germany**
Signature		Date	
FULL NAME OF INVENTOR	FAMILY NAME **KOWALSKI**	FIRST GIVEN NAME **Bernd**	SECOND GIVEN NAME
RESIDENCE & CITIZENSHIP	CITY & ZIP CODE **D-57072 Siegen**	STATE & OR FOREIGN COUNTRY **Germany** DEX	COUNTRY OF CITIZENSHIP **Germany**
POST OFFICE ADDRESS	POST OFFICE ADDRESS **Am Bastenberg 4**	CITY & ZIP CODE **D-57072 Siegen**	STATE OR FOREIGN COUNTRY **Germany**
Signature		Date 25.01.2000	

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: ASSISTANT COMMISSIONER FOR PATENTS
Washington, D.C. 20231

U.S. APPLICATION NO.	FIRST NAMED APPLICANT	ATTY DOCKET NO
09/485408	WILHELM S	2345/115

INTERNATIONAL APPLICATION NO
PCT/EP98/04424

I.A. FILING DATE	PRIORITY DATE
16 JUL 98	06 AUG 97

KENYON & KENYON
ONE BROADWAY
NEW YORK, NY 10004

DATE MAILED 21 APR 2000

NOTIFICATION OF ACCEPTANCE OF APPLICATION UNDER 35 U.S.C. 371 AND 37 CFR 1.494 OR 1.495

1. The applicant is hereby advised that the United States Patent and Trademark Office in its capacity as ☐ a Designated Office (37 CFR 1.494), ☒ an Elected Office (37 CFR 1.495), has determined that the above identified international application has met the requirements of 35 U.S.C. 371, and is **ACCEPTED** for national patentability examination in the United States Patent and Trademark Office.

2. The United States Application Number assigned to the application is shown above and the relevant dates are:

07 FEB 2000	07 FEB 2000
35 U.S.C. 102(e) DATE	DATE OF RECEIPT OF 35 U.S.C. 371 REQUIREMENTS

A Filing Receipt (PTO-103X) will be issued for the present application in due course. **THE DATE APPEARING ON THE FILING RECEIPT AS THE "FILING DATE" IS THE DATE ON WHICH THE LAST OF THE 35 U.S.C. 371(C) REQUIREMENTS HAS BEEN RECEIVED IN THE OFFICE. THIS DATE IS SHOWN ABOVE.** *The filing date of the above identified application is the international filing date of the international application (Article 11(3) and 35 U.S.C. 363).* Once the Filing Receipt has been received, send all correspondence to the Group Art Unit designated thereon.

3. ☒ A request for immediate examination under 35 U.S.C. 371(f) was received on 07 FEB 2000 and the application will be examined in turn.

4. The following items have been received:
- ☒ U.S. Basic National Fee.
- ☒ Copy of the international application in:
  - ☒ a non-English language.
  - ☐ English.
- ☒ Translation of the international application into English.
- ☒ Oath or Declaration of inventors(s) for DO/EO/US.
- ☐ Copy of Article 19 amendments. ☐ Translation of Article 19 amendments into English.
  The Article 19 amendments ☐ have ☐ have not been entered.
- ☒ The International Preliminary Examination Report in English and its Annexes, if any.
- ☒ Copy of the Annexes to the International Preliminary Examination Report (IPER).
  - ☒ Translation of Annexes to the IPER into English.
  - The Annexes ☒ have ☐ have not been entered.
- ☒ Preliminary amendment(s) filed 07 FEB 2000 and _____.
- ☒ Information Disclosure Statement(s) filed 07 FEB 2000 and _____.
- ☒ Assignment document.
- ☒ Power of Attorney and/or Change of Address.
- ☒ Substitute specification filed 07 FEB 2000.
- ☐ Verified Statement Claiming Small Entity Status.
- ☒ Priority Document.
- ☒ Copy of the International Search Report ☒ and copies of the references cited therein.
- ☐ Other:

Applicant is reminded that any communication to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above. (37 CFR 1.5)

Winston M Alvarado
Telephone: 703-305-6421

FORM PCT/DO/EO/903 (December 1997)